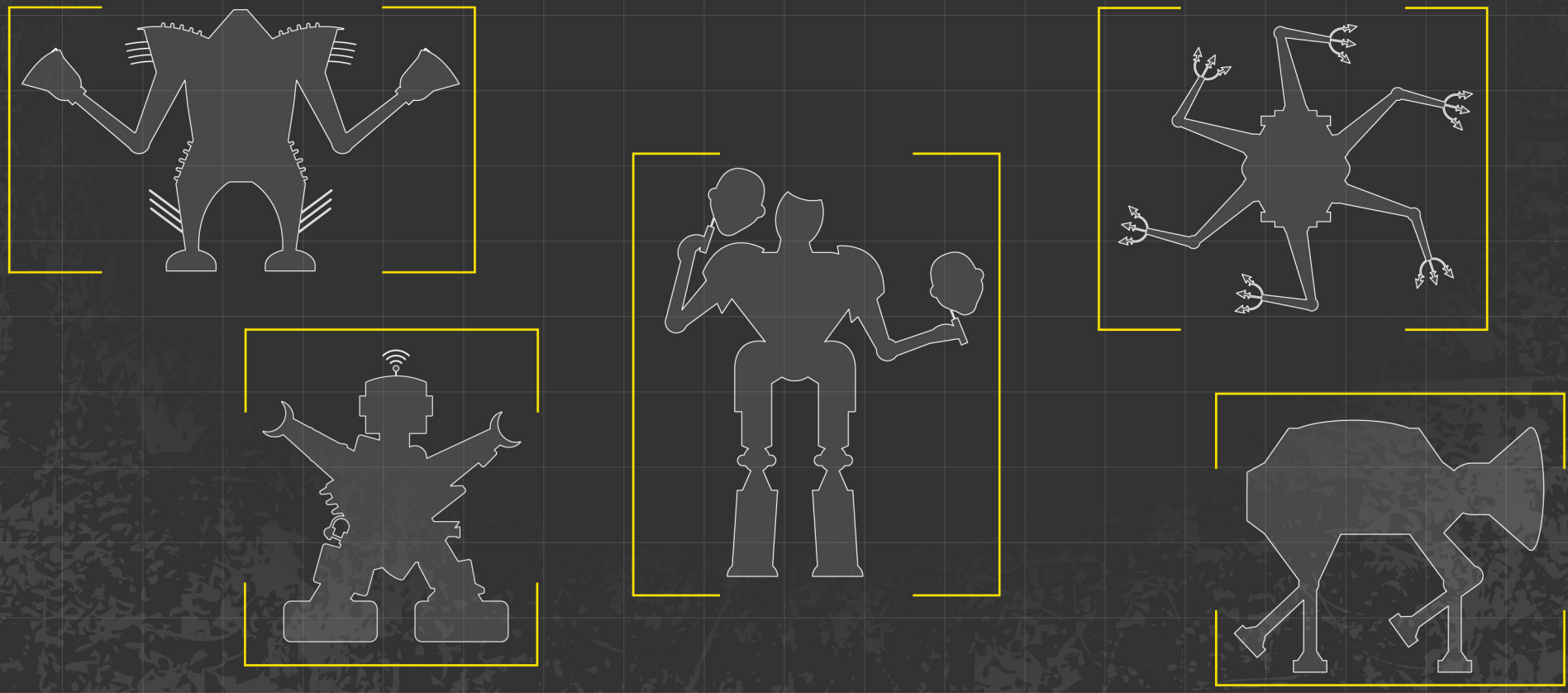
EBOOK

dyn.com 603 668 4998 @dyn

ORACLE + Dyn

DARK BOT SURVIVAL GUIDE

Strategies for Understanding the Evolving Web Security Threat Landscape



Dark Bot Survival Guide

Strategies for Understanding the Evolving Web Security Threat Landscape

We live in a world where bot technology is becoming increasingly sophisticated and dangerous. Online bot activity has outstripped human activity and now makes up more than half of all Internet traffic, and this number continues to grow.

The rapidly expanding and advancing technologies have revealed weak spots in traditional security measures. Differentiating between human and bot is becoming harder and harder to confirm. There is also an ever-widening pool of threat actors and a rapidly growing number of devices in the IoT landscape. Anyone with web-facing assets is left with the daunting task of picking the difference between good bots, human activity, and malicious bad bots.

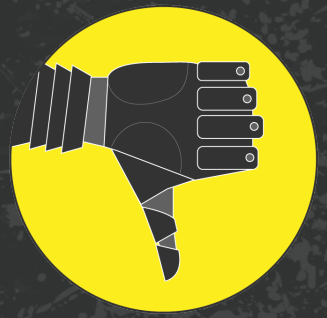
Hackers use bots to execute a range of damaging, fraudulent, and unwanted activity. Everything from spam and content scraping, to distributed denial of service attacks (DDoS) and API outages. Bad bots can cause serious damage, significant downtime, and irreparable commercial loss.

Of course, there are good bots and they are an essential part of the Internet. They help run automated tasks, share information, facilitate communication, and analyze information to improve content and enhance your customers' online experience. But balance is key. You need good bots, but too much good bot traffic can also negatively impact the user experience.

The bottom line is that businesses must have a sound survival strategy to deploy technology that keeps them one step ahead of the threat by identifying and eliminating hostile bot traffic. At the same time, businesses also must keep legitimate and business-critical bot traffic flowing. The need is for innovation, advanced technologies, and expertise that can outsmart the malicious actors and secure your assets, data, and customers.

IDENTIFY YOUR BOTS

BAD BOTS



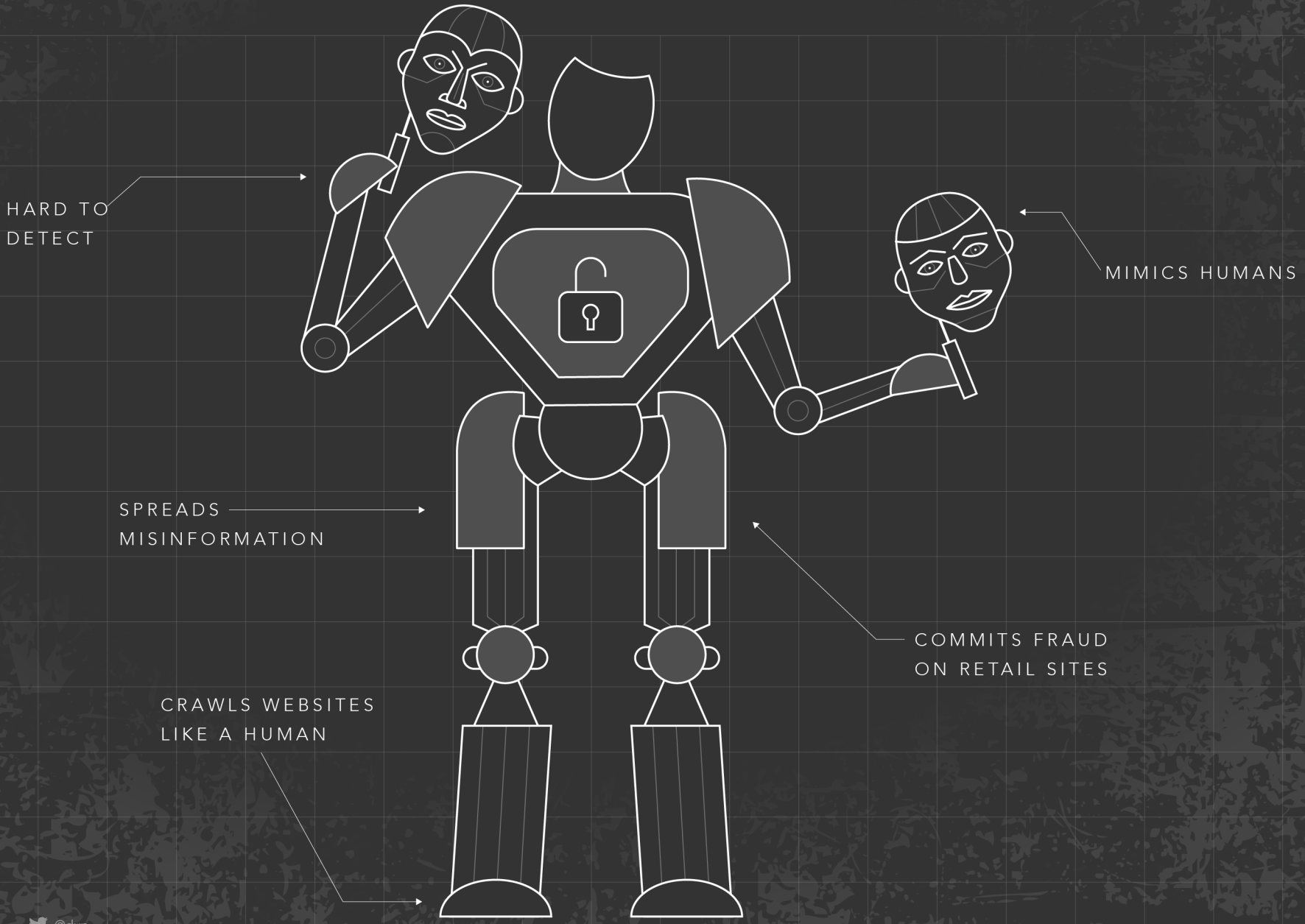
- Impersonator Bots
- Scraper Bots
- Click/Ad Fraud Bots
- Spam/Email Bots
- Botnets

GOOD BOTS

- Spider Bots
- Media/Data Bots
- Copyright Bots

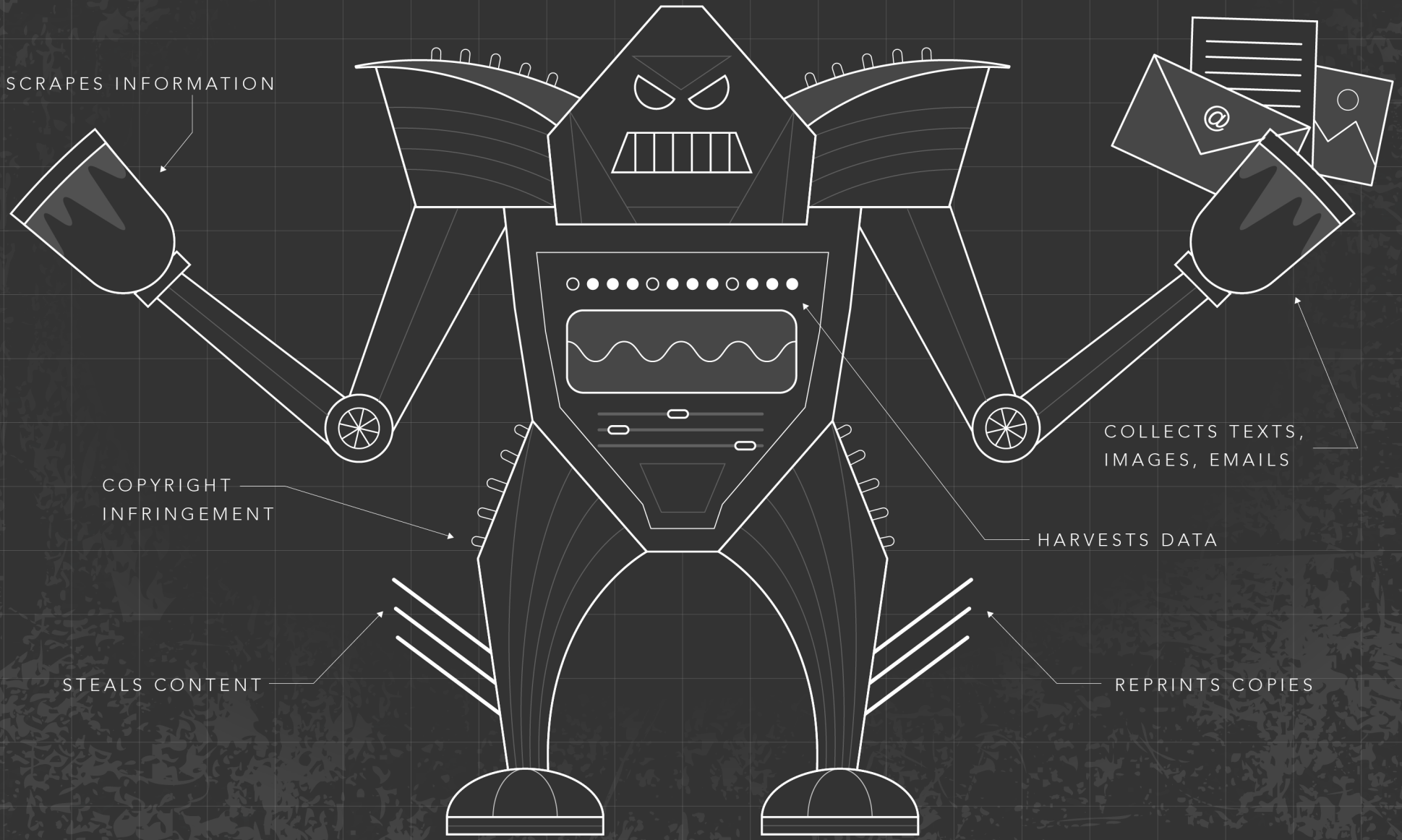
1 IMPERSONATOR BOTS

These hard-to-detect bots closely mimic online human activity. They crawl websites acting like humans and bypass regular site security to execute attacks like jamming shopping carts on retails sites or spreading misinformation.



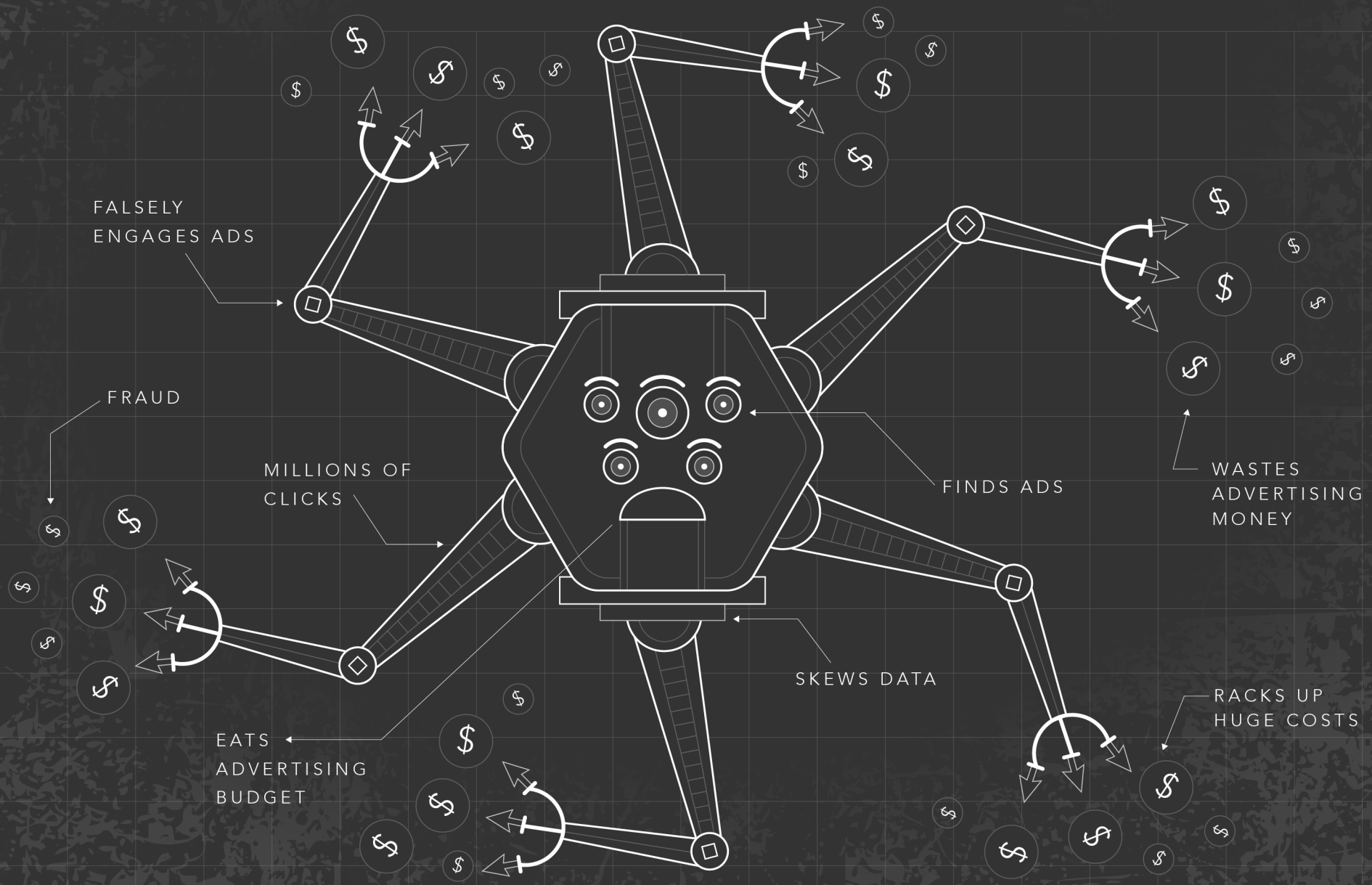
2 SCRAPER BOTS

Scraper Bots steal content. They harvest website content such as text, images, email addresses, and other information to be consolidated and sold to other sites and illegitimate listing sources. They can also be used to undermine pricing strategies or steal original content from a site and reprint it elsewhere without permission.



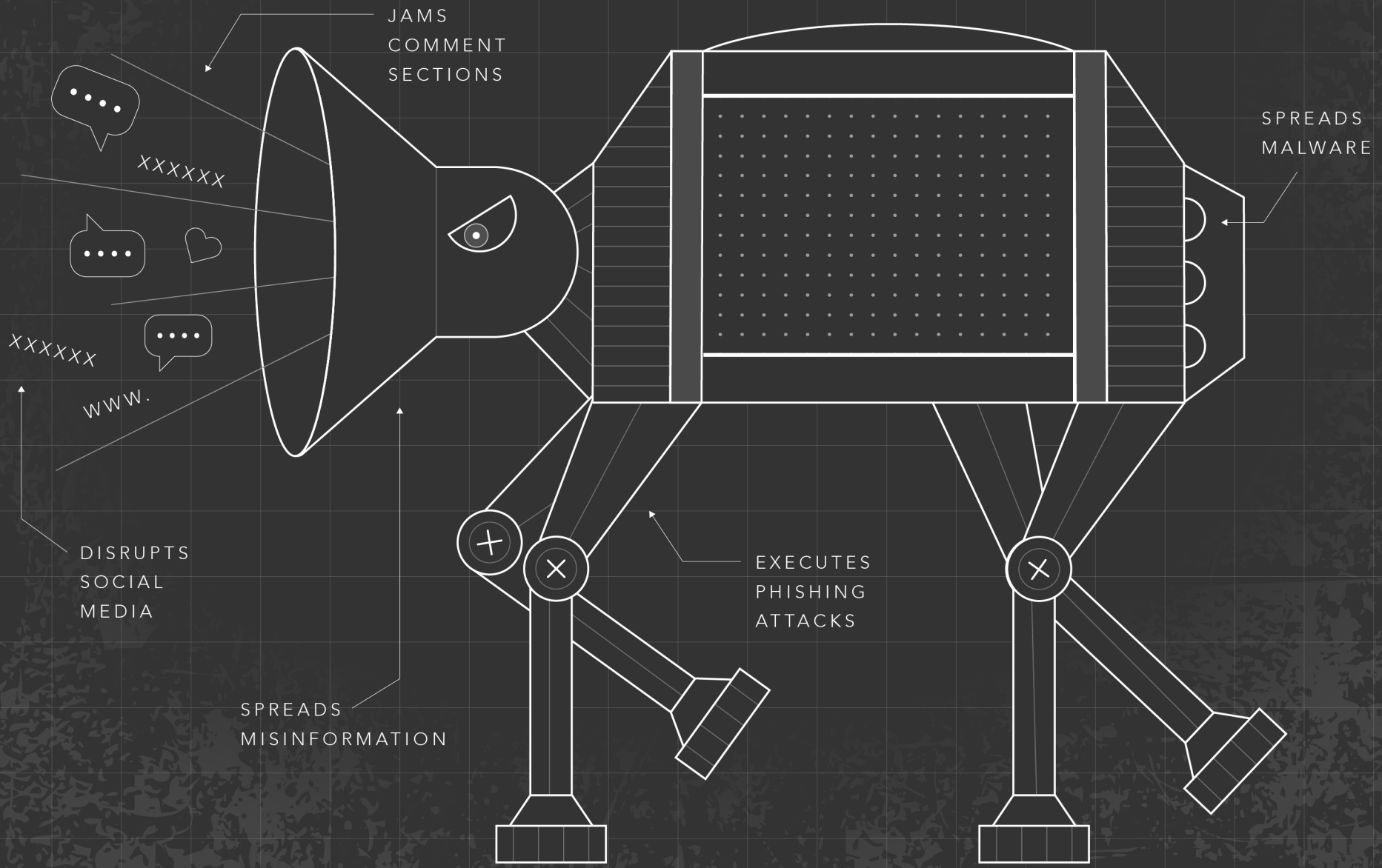
3 CLICK/AD FRAUD BOTS

Particularly devious, Click/Ad Fraud Bots are designed to engage with paid advertising to skew data and waste ad money. These bots can be programmed to click on ads millions of times, racking up huge charges for anyone who paid for the ad.



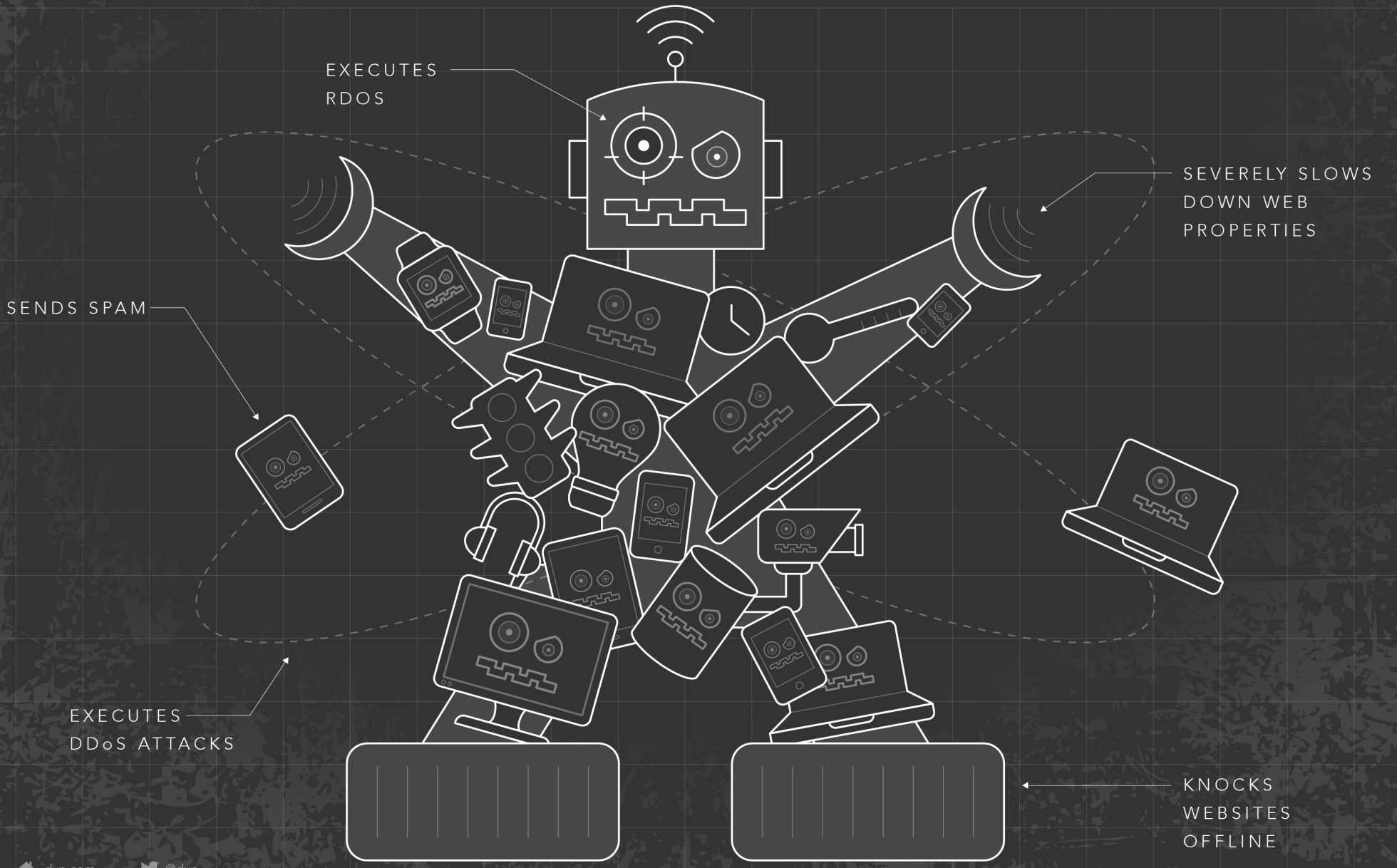
4 SPAM/EMAIL BOTS

These bots are more than a nuisance; they can cause serious damage. They target community portals, blog comment sections and social media channels. They are leveraged to disseminate false information or spread links loaded with malware and/or fraudulent forms used to dupe unsuspecting users into giving away their information.



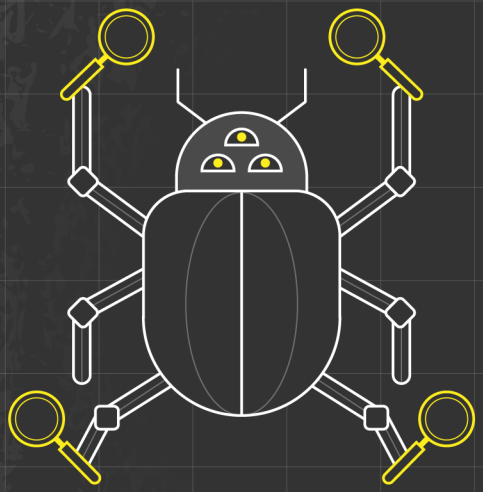
5 BOTNETS

Botnets are perhaps the most dangerous of all. If left unprotected, anything with an Internet connection, from a laptop to an IoT device, can be turned into a "zombie bot" without the user ever knowing. These zombie bots are then gathered in a gigantic swarm known as a Botnet. A hacker will then direct a Botnet at a single target, overflowing the target's resources and knocking them offline, AKA a DDoS attack.



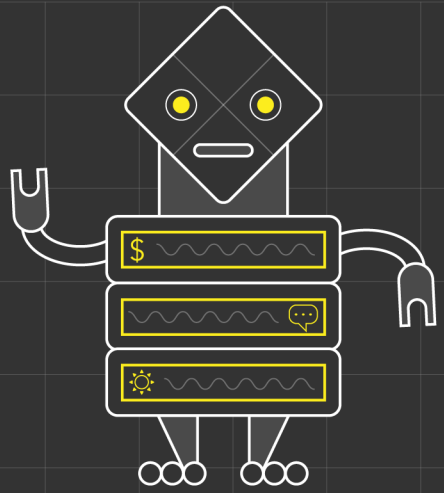
6 GOOD BOTS

It may appear that the simplest and safest solution to the bot epidemic would be to block all bot traffic entirely. However, measures that drastic will do more harm than good to your web properties and your business. Some bots play a positive role in the integrity and success of your organization.



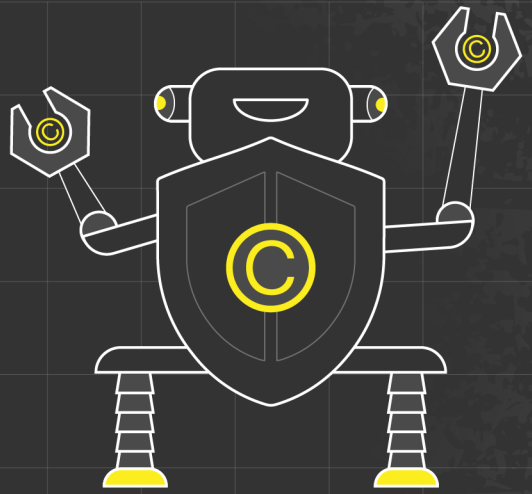
Spider Bots

Spider Bots are used by major search engines to crawl websites and perform analysis used for SEO ranking. These bots boost your site's search results by gathering data on the amount of original content, pictures and hyperlinks. Blocking these bots entirely leads to a drop in SEO and risks your site not appearing in search results at all.



Media/Data Bots

These bots source data and give updates on weather, news, finance, and other real-time information. They can also be used to monitor and censor online chat rooms and IM programs.



Copyright Bots

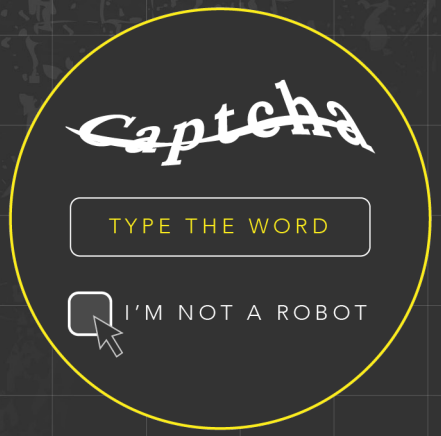
Copyright Bots scour the web searching for content and making sure none of yours has been plagiarized elsewhere.

These bots are necessary, but remember that they also need monitoring. Too much good bot traffic can impact human user engagement. Your security solution must be able to recognize good bot traffic and manage it before it affects the human experience.

SECURITY PRIORITIES

The key to a strong bot strategy is twofold: identification and management. For tactical methods, the immediate priorities are to identify the dark bots and mitigate them. There are a number of techniques available to help deploy your strategy.

Identification Methods

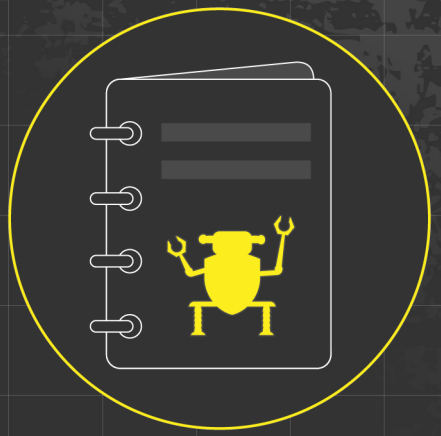


CAPTCHA

is a challenge intended to differentiate between computers and humans. Users are asked to identify a series of letters and number or click on a set of pictures displaying a specific image. Scripted bots are unable to repeat the words and numbers and are not able to solve the CAPTCHA, whereas humans can.

JavaScript Challenge

is sent to every client, attacker, and real user. Legitimate browsers will pass the challenge without the user's knowledge while bots, which are typically not equipped with JavaScript, will fail and be blocked.



Good Bot Whitelisting

gives users the ability to recognize and remember good bots and automatically allow them access.

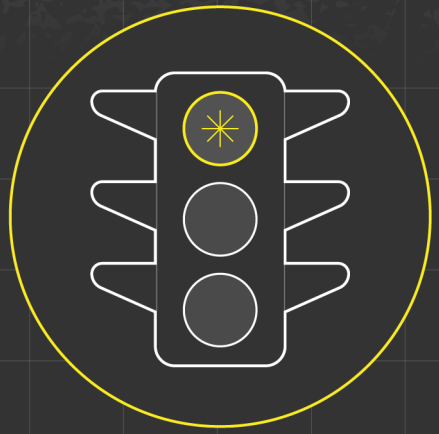
SECURITY PRIORITIES

Identification basics are good enough for general security and management, but the dark bot threat is becoming more and more complex. Enterprises also need advanced methods to mitigate emerging and increasingly sophisticated technologies.

Advanced Mitigation Methods

Human Interaction Challenge

identifies normal usage patterns for each web application based on legitimate user/visitor behavior analysis and provides customizable security postures for bots that deviate from the standard usage behavior, activity, or frequency.



Bot Traffic Shaping

is a traffic control mechanism used to detect and delay traffic created by suspicious bots, while at the same time prioritizing and whitelisting authorized traffic.

Device Fingerprinting

generates a hashed signature of both virtual and real browsers based on 50+ attributes. These proprietary signatures are then leveraged for real-time correlation to identify and block malicious bots.

Essential for any modern defense strategy is the use of artificial intelligence (AI) and machine learning. These advanced technologies can detect extremely subtle and minute patterns that otherwise can go undetected.

WHAT DOES YOUR BOT SURVIVAL STRATEGY LOOK LIKE?

As malicious bots continue to transform and develop, the threat against web security continues to grow in scope and severity. It's critical to preserve and protect your valuable web applications at all times.

With a mix of monitoring and proactive management, you can develop a survival strategy and implement defense mechanisms to stop malicious bot activity in its tracks.

Does your bot survival strategy do this?

- Detect and block malicious bot traffic
- Allow and manage good bots
- Include configurable challenge/detection techniques
- Redirect unwanted bot traffic to preconfigured pages
- Provide visual bot classifications
- Conserve bandwidth and web resources
- Incorporate AI and machine learning

LEARN MORE ABOUT BUILDING YOUR SURVIVAL STRATEGY

https://dyn.com/bot-manager/